Journal of Korea Multimedia Society Vol. 11, No. 4, April 2008(pp. 504-515)

유비쿼터스 컴퓨팅 환경에서 이기종 네트워크간 안전한 키 관리 기술에 관한 연구

문종식†, 이임영††

요 약

유선 네트워크의 빠른 전송속도 및 다양한 서비스와 무선의 편리성 및 이동성이 결합되어 새로운 서비스 영역을 창출하고 사용자와 서비스 제공자 모두에게 새로운 변화를 가져올 신기술로 유/무선 통합 시대가 전개되고 있다. 유/무선 통합 서비스 중에서 네트워크의 통합은 이기종 네트워크간 연동에 의한 네트워크 융합과 네트워크상에서 전송기술간 융합으로써 매주 중요한 부분을 차지하고 있다. 이러한 상황 속에서 이기종 네트워크의 융합은 서로 다른 네트워크의 융합으로 인해 기존의 보안 기술 및 통신 기술을 그대로 적용하기가 매우 어려우며, 보안 측면에서도 많은 취약점을 내포하고 있다. 기존의 동종 네트워크에서 사용자의 인증 및 키 관리와는 다르게 이기종 네트워크간의 사용자 인증 및 키 관리는 새로운 기술이 필요한 실정이며 또한 동종 네트워크에서 이기종 디바이스간의 보안 기술 확립은 매우 중요한 사항이라 할 수 있다. 본 논문에서는 이기종 네트워크 환경에서의 안전하고 효율적인 키 관리를 제안하여, 이기종 네트워크 디바이스간의 안전한 통신을 제공 할 수 있다.

A Study on Secure Key Management Technology between Heterogeneous Networks in Ubiquitous Computing Environment

Jong-Sik Moon†, Im-Yeong Lee††

ABSTRACT

Fast transmission speeds and various wired network services have been combined with the convenience and mobility of wireless services. The combination of wired/wireless technologies is spreading rapidly since it enables the creation of new services and provides new features to both users and service providers. In such wired/wireless integrated services, network integration is very important because such systems are integrated by a linkage between heterogeneous networks and they involve an integration of transmission technologies across networks. In this situation, existing security and communication technologies are unsuitable since the network are integrated with heterogeneous networks. The network may also have several security flaws. In existing homogeneous networks, user authentication and key management between heterogeneous networks are required for these new technologies. The establishment of security technologies for heterogeneous devices is a very important task between homogeneous networks. In this paper, we propose a secure and efficient key management system for a heterogeneous network environment. Our system provides secure communications between heterogeneous network devices.

Key words: ID-Based(아이디 기반), Heterogeneous Network(이기종 네트워크), Key Management(키 관리), Authentication(인증)

※ 교신저자(Corresponding Author) : 이임영, 주소 : 충남 아산시 신창면 읍내리 순천향대학교(336-745), 전화 : 041) 542-8819, FAX : 041)530-1548, E-mail : imylee@sch. ac.kr
접수일 : 2007년 8월 16일, 완료일 : 2007년 11월 28일
† 준회원, 학생회원, 순천향대학교 컴퓨터학과
(E-mail : comnik528@sch.ac.kr)
†† 종신회원, 순천향대학교 컴퓨터학부 교수
※ "본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

1. 서 론

유선 네트워크의 빠른 전송속도 및 다양한 서비스와 무선의 편리성 및 이동성이 결합되어 새로운 서비스 영역을 창출하고 사용자와 서비스 제공자 모두에게 새로운 변화를 가져올 신기술로 유/무선 통합 시대가 전개되고 있다[1,2]. 기존의 유선과 무선으로 구분되었던 서비스가 유/무선 통신망의 기술 발전으로 각국의 정부와 통신 사업자들은 차세대 네트워크(Next Generation Network, NGN)시대에 대비하여 통신정책의 변화와 새로운 서비스 개발 등의 노력을 하고 있다. 유/무선 통합 서비스 중에서 네트워크의 통합은 이기종 네트워크간 연동에 의한 네트워크 융합과 네트워크상에서 전송기술간 융합으로써 매우 중요한 부분을 차지하고 있다. 최근 유/무선 통합 서비스에 대한 수요가 폭발적으로 증가할 것이라는 예상에 따라 이기종 네트워크간의 서비스는 수많은 관련 산업의 창출 등 정보통신 산업의 활성화와 국가 경쟁력 제고에 주도적인 역할을 담당할 것이다. 뿐만 아니라 국내 핵심 정책 중 유/무선 네트워크 통합이 선정되고 연구 개발됨으로써 이기종 네트워크간의 서비스는 많은 영향을 미칠 것이라고 예상하며 산업화가 가속화 되고 있다. 그러나 이기종 네트워크의 융합은 서로 다른 네트워크의 융합으로 인해 기존의 보안 기술 및 통신 기술을 그대로 적용하기가 매우 어려우며, 보안 측면에서도 많은 취약점을 내포하고 있다. 이로 인해 네트워크간 융합 시 네트워크 보안과 사용자에 대한 인증 및 키 관리가 중요한 연구 과제들 중의 하나로 떠오르고 있으며, 기존의 동종 네트워크에서 사용자의 인증 및 키 관리와는 다르게 이기종 네트워크간의 사용자 인증 및 키 관리는 새로운 기술이 필요한 실정이다.

따라서 본 제안 방식은 이기종 네트워크 환경에서의 안전하고 효율적인 키 관리를 제안하여 이기종 네트워크 디바이스간의 안전한 통신을 제공 할 수 있도록 하고자한다. 그리고 기존의 대칭키 기반 방식[3,4]과 공개키 기반 방식을 분석하고 보안 요구 사항을 도출하여 안전하고 효율적인 이기종 네트워크간의 키 관리를 제안하였다. 본 논문의 구성은 다음과 같다. 2장에서는 연구 배경에 대하여 알아보며, 3장에서는 기존 방식에 대하여 알아본다. 4장에서는 제안 방식에 대하여 설명하며, 5장에서는 2장의 보안 요구 사항, 공격에 따른 요구 사항 및 통신에 따른 효율성으로 제안 방식을 분석하고 마지막으로 6장에서는 결론 및 향후 연구 방향으로 마치도록 한다.

2. 연구 배경

본 장에서는 보안 요구 사항에 대하여 알아보고, 이기종 네트워크간의 키 관리 기술의 기반이 되는 VPN 및 IKEv2와 신원기반 시스템의 개요에 대하여 살펴본다.

2.1 보안 요구 사항

이기종 네트워크에서는 기존의 요구 사항 외에 이기종 네트워크 특성에 따라 단말간 상호 인증 및 단대단 보안 등이 제공되어야 하며, 제 3자의 공격으로부터 노출되어 있어 보안상 취약점을 내포하고 있다. 이에 따라 이기종 네트워크간의 전송되는 메시지 및 통신은 다음과 같은 요구 사항을 고려해야 한다.

가. 일반적인 보안 요구 사항

- 기밀성(Confidentiality) : 통신에 사용되는 데이터는 정당한 객체만이 확인할 수 있어야 하며, 데이터의 출처와 목적지, 횟수, 길이, 또는 통신선로 상의 트래픽 특성에 대하여 공격자가 알지 못하게 해야 한다. 기밀성은 정보를 해석할 수 없도록 암호화를 통해서 이루어진다.
- 무결성(Integrity) : 정보 시스템에 저장되어 있거나 네트워크를 통해 전송되는 데이터가 위변조 되거나 파괴되지 않도록 해야 한다. 만약 위조, 삭제 및 변조가 되었다면 그 사실을 확인할 수 있어야 한다. 전송된 데이터의 무단 변경을 감지할 수 있게 하기위해 전자 서명 등을 이용한다.
- 인증(Authentication) : 인증 서비스는 통신이 기밀성을 갖도록 보증하는 것이 중요하다. 서비스를 이용하고자 접근하는 사용자가 전송한 메시지 또는 전자문서의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 접근제어(Access Control) : 정보 자원에 대한 읽기나 변경 등의 모든 접근 행위에 대해 그 권한을 명백히 구분해 허가되지 않은 접근 시도를

사전에 차단할 수 있도록 하는 통제가 필요하다. 시스템에서는 운영체제의 접근통제 기능을 사용하며 네트워크에서는 침입차단 시스템을 사용해서 접근통제 수준을 높일 수 있다. 또한 서비스 이용에서 정당하지 않은 사용자는 서비스를 이용할 수 없다.

- 부인 봉쇄(Non-repudiation) : 합법적인 객체들 사이에서 송·수신된 정보는 이 정보를 송·수신한 객체가 이 사실을 부인할지라도 당사자 및 제 3자에 의해 확인 될 수 있어야 한다. 거래 당사자간에 정보 제공 부인을 방지하는 것이다. 특히 네트워크를 이용한 전자상거래나 법률 행위에서는 매우 중요하다. 부인 방지는 무결성 보장과 마찬가지로 전자서명에 의해 해결할 수 있다.

나. 이기종 네트워크에서의 보안 요구 사항

- 상호 인증(Mutual Authentication) : 상호 인증은 통신하는 객체간에 양방향으로 각각의 개체를 인증하는 것이다. 이기종 네트워크에서는 다양한 객체간 통신이기 때문에 상호간의 인증이 필요하다.
- 단대단 보안(End-to-End Secrecy) : 단대단 보안의 경우 암호화 과정은 두 종단 시스템에서 수행되며, 출처 호스트나 터미널이 데이터를 암호화한다. 데이터는 암호화된 형식으로 네트워크를 통하여 목적지 터미널이나 호스트로 변경없이 전송된다. 이기종 네트워크에의 단말간 통신은 단대단 보안이 제공되어야 한다.

다. 공격에 따른 요구 사항

- 도청 공격(Eavesdropping Attack) : 통신 채널에서 전송되는 데이터가 제 3의 공격자에게 노출될 수 있기 때문에 도청 공격에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 비밀값을 유추할 수 없도록 해야 한다.
- 재전송 공격(Replay Attack) : 프로토콜상에서 유효 메시지를 골라 복사한 후 나중에 재전송함으로써 정당한 사용자로 가장하는 공격이다. 시간이나 순서에 따른 유효성을 검출할 수 있도록 순서 번호나 타임스탬프, 또는 도전/응답 등으로 방어할 수 있다. 통신 중에 전송되는 데이터를 제 3자가 획득하여 메시지를 재전송함으로써 인증 받는 것을 막을 수 있어야 한다.
- 위장 공격(Impersonation Attack) : 안전하지 않은 통신로 상에서는 악의적인 제 3자가 정당한 사용자처럼 위장하여 인증 및 서비스를 제공받을 수 있다. 따라서 제 3자가 정당한 사용자처럼 접근하는 것을 막아야 한다.
- 패스워드 추측 공격(Password Guessing Attack) : 안전하지 않은 통신로 상에서 악의적인 제 3자가 전송되는 메시지를 분석하여 패스워드를 추측할 수 있다. 따라서 통신 중에 전송 되는 메시지를 분석하여 패스워드를 추측하는 것을 막아야한다.

2.2 VPN

VPN(Virtual Private Network)은 공공 인터넷에서 보안은 물론, 한 회사 내 그리고 다른 회사간의 통신에서의 비용효과를 제공하기 위해서 세계적으로 개발되고 있으며, 통상적인 사설망들은 대규모 조직들에 의해서 운영되어 진다. 과거의 VPN은 개인 장비를 사용해서 내부 트래픽을 운반 하였으며, 이렇게 하는 것은 일반적으로 외부 사용자들이 접근하기 어렵다. 폐쇄되고 빈틈없는 환경 속에서 전통적인 사설망은 일반적으로 안전하다고 생각되어 왔으나 오늘날의 사설망들은 새로운 비즈니스 모델을 향해 발전하고 있다. 확장된 사설망은 물리적으로 분리된 인트라넷들을 공공의 인터넷을 통해 서로 연결하고 다른 회사와의 통신은 사업상 필연적으로 필요하다. 이 새로운 비즈니스 모델은 전통적인 사설망 모델에는 존재하지 않는 보안 노출이 존재한다. VPN의 디자이너와 운영자들은 노출된 보안을 이해하고 보호할 수 있어야 한다. IPSec(IP Security Protocol)은 이러한 VPN의 문제점을 해결할 수 있는 방안으로 사용되고 있다. VPN, 정확히 말해 VPDN (Virtual Private Dial-up Network)은 터널링 기법이라 대변될 만큼 VPDN에 있어서 터널링 기술은 중요하다. 터널링 프로토콜은 캡슐화, 전송, 디캡슐화 과정을 포함하며, 터널링 프로토콜은 먼저 라우팅 정보를 포함하는 추가헤더정보로 프레임을 캡슐화하여 전송한다. 캡슐화된 프레임은 추가 헤더정보 내의 라우팅 정보를 기반으로 공중망을 경유하여 터널 엔드포인트로 전송된다. 캡슐화된 프레임이 망의 목적지에 도달하면 디캡슐화 되어 최종 목적지로 향한다. 터널링

기술은 새로운 기술이 아니라 이미 존재하였던 기술로서, SNA(System Network Architecture) 또는 IPX(novell Interwork Packet Exchange) 트래픽을 인터넷으로 전송할 때 UDP(User Datagram Protocol)와 IP(Internet Protocol) 헤더로 캡슐화하여 전송하는 것을 예로 들 수 있다. 현재 터널을 생성하기 위한 프로토콜들은 PPP(Point-to-Point Protocol), PPTP(Point-to-Point Tunneling Protocol), L2FP(Layer 2 Forwarding Protocol), L2TP(Layer 2 Tunneling Protocol), IPSec, VTP(Virtual Tunneling Protocol), Socks, SSL(Secure Sockets Layer) 등과 같이 매우 다양하며, 여러 응용 서비스에 적용할 수 있다[5,6].

2.3 IKEv2

IKEv2(Internet Key Exchange Version2)는 IKE의 후속 프로토콜로서 IETF IPSec Working Group에서 여러 가지 IKE의 문제점들을 보완하기 위해 2001년 8월부터 논의된 프로토콜이다[7]. IKEv2는 IKE의 대부분의 속성들을 유지하면서 효율성과 안전성, 강건성, 유연성을 증대시키는 방향으로 재구성되었다[8]. IKEv2는 IKE의 2단계 Phase 방식과 SA(Security Association) 협상방식을 계승한다. 반면에 인증방식을 디지털 서명방식 하나로 간소화 했으며, Phase 1에서도 IPSec-SA 협상이 가능하도록 했다. DoS(Denial of Service) 공격에 대응하는 메커니즘으로 공격이 예상되면 Cookie 정보를 가진 추가 메시지를 교환 하도록 되어 있다. Phase 1은 기본적으로 4개의 메시지로 구성되며 첫 번째 메시지 쌍인 IKE_SA_INIT에서는 IKE_SA의 협상 및 설정에 필요한 D-H(Diffie- Hellman) 키 교환을 수행하고 Nonce 값과 필요한 파라미터들을 교환한다. IKE_SA_INIT이 완료된 이후의 메시지는 설정된 IKE_SA에 의해 암호학적 보호를 받게 된다. 두 번째 메시지 쌍인 IKE_AUTH에서는 상호 인증을 위한 식별 정보와 인증 정보를 교환하고 Child-SA 설정에 필요한 파라미터들을 협상한다. 이 때 Child-SA를 협상함으로써 IPSec-SA의 생성지연을 최소화 할 수 있다. Subsequence Exchange는 두 개의 메시지로 구성되며, Child-SA를 설정하거나, 프로토콜 수행 중에 발생한 오류정보 및 이벤트 발생 정보 등을 교환 한다. 또한 SA의 재설정에도 사용된다. Subsequence Exchange는 그 용도에 따라 Child-SA를 설정하거나 기존 SA를 재설정하는 Create-Child-SA와 오류정보 및 이벤트 발생정보를 교환하기 위한 정보 교환으로 구분한다.

IKEv2는 Phase 1 및 Phase 2 에서 D-H값을 교환할 때마다 매번 새로운 값을 교환한다고 가정하면 PFS(Perfect Forward Secrecy)가 보장될 수 있다. 하지만 서로 다른 IKE SA 간에 같은 D-H 값을 재사용할 수 있도록 하여 불안전한 PFS를 허용하였다. Identity 보호에 있어서 개시자에 대해 수동적인 보호를 하고, 응답자에 대해 적극적인 보호를 하지만 개시자가 먼저 Identity를 보내기 때문에 공격자가 응답자를 가정하여 공격하는 적극적 공격에는 보호될 수 없다. 또한 SA에 있어서 호환성을 가지게 하는 장점은 있으나, 결국 프로토콜을 복잡하게 하는 단점을 갖는다[9].

2.4 신원기반 시스템

신원기반 공개키 암호시스템은 1984년 Shamir가 처음으로 제안하였다[10]. 이 시스템에서 사용자의 공개키는 전자우편주소나 주민등록번호처럼 그 사용자의 잘 알려진 신원정보로부터 생성할 수 있다[4]. 따라서 기존 PKI 기반 공개키 시스템과 달리 공개키와 사용자를 바인딩하여 주는 인증서가 필요 없다. 즉, 통신하고자 하는 상대방이나 제 3의 서버에게 문의하지 않고 상대방의 신원을 알고 있다면 상대방의 공개키를 생성할 수 있다. 이것이 신원기반 암호시스템의 가장 큰 장점이다. 겹선형 쌍함수(Bilinear Pairing)는 타원곡선 상의 이산대수 문제를 유한체상의 이산대수 문제로 축소시켜 그 어려움을 줄여 타원곡선 암호시스템을 공격하는 도구로 원래 제안되었다. 최근에는 공격 도구가 아닌 정보보호를 위한 암호학적 도구로 사용되고 있다. 겹선형 쌍함수는 다른 말로 겹선형 사상(Bilinear Map)이라 한다. 이 절에서는 다음과 같은 표기법을 사용하며, 이 Map의 정의는 다음과 같다.

- q : 매우 큰 소수
- G_1 : 위수가 q인 타원곡선 위의 덧셈군
- G_2 : 위수가 q인 유한체 위의 곱셈군
- $P, Q, R \in {}_R G_1$
- $a, b, c \in {}_R Z_q^*$

[정의 1.] 다음과 같은 특성을 만족하는 $\hat{e}: G_1 \times G_1 \rightarrow G_2$를 사용하는 Admissible Bilinear Map이라 한다.

- 겹선형(Bilinear) : 임의의 P, Q, R에 대하여 다음이 성립해야 한다.
  - $\hat{e}(P, Q+R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$
  - $\hat{e}(P+Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$
- 비퇴화성(Non-Degenerate) : G_1의 모든 쌍 P, Q에 대하여, $\hat{e}(P, Q)$는 G_2의 항등원이 아니어야 한다.
- 계산가능성(Computable) : 임의의 P, Q에 대하여 $\hat{e}(P, Q)$를 계산할 수 있는 효율적인 알고리즘이 존재해야 한다.

겹선형 사상의 특성에 의해 다음이 성립한다.

$$\hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b$$
$$= \hat{e}(P, Q)^{ab} = \hat{e}(abP, Q) = \hat{e}(P, abQ)$$

이 사상 때문에 타원곡선 상에서 D-H 결정 문제는 다음 식을 통해 쉽게 해결할 수 있다.

$$\hat{e}(aP, bQ) = \hat{e}(cP, P) \Rightarrow ab = c$$

따라서 겹선형 사상을 암호학적 도구로 사용하는 많은 암호프로토콜에서는 다음 문제의 어려움에 기반하고 있다.

[정의 2.] (BDHP, Bilinear Diffie-Hellman Problem) G_1의 원소 P, aP, bP, cP가 주어졌을 때, $\hat{e}(P, P)^{abc}$를 계산하는 문제를 말한다.

이 문제는 타원곡선 이산대수 문제를 해결할 수 있으면 해결할 수 있다. 예를 들어 aP로부터 a를 계산할 수 있으면 $\hat{e}(bP, cP)^a$를 통해 $\hat{e}(P, P)^{abc}$를 계산할 수 있다. 뿐만 아니라 이 문제는 타원곡선 D-H 문제를 해결할 수 있으면 해결할 수 있다. 예를 들어 aP, bP로부터 abP를 계산할 수 있으면 $\hat{e}(abP, cP)$를 통해 $\hat{e}(P, P)^{abc}$를 계산할 수 있다. 본 연구에서는 이기종 디바이스간 키 설립 단계에서 키 설립 비밀 값을 생성하는데 Admissible Bilinear Map을 기반으로 진행하였다.

3. 기존 연구

이기종 네트워크에 관한 기존 연구의 각 방식에 대하여 알아보고 방식별 특징 및 장/단점에 대하여 언급한다.

3.1 ID 기반 인증 키 교환 방식

ID 기반 인증 키 교환 방식은 이기종 무선 접속의 안전성을 위해 신원기반 인증과 AKE(Authentication Key Exchange)프로토콜을 제안하였으며, CK (Canetti and Krawczyk) Model을 사용하여 이상적이고 안전한 키 교환 프로토콜을 처음 제안 하였다[11]. ID 기반 인증 키 교환 방식에서는 Shamir에 의해 처음 제안된 신원 기반 공개키 암호 시스템[10]을 이용하여 효율적인 AKE 프로토콜을 디자인하였다. 인증서가 필요 없는 신원 기반 공개키 시스템은 공개키 암호의 장점을 그대로 가지면서 전통적인 인증서 기반 공개키 암호 시스템의 복잡성을 감소 시켰다. 따라서 ID 기반 인증 키 교환 프로토콜은 사용자 측면에서 계산의 로드를 주로 고려하여 다른 방식들보다 계산량에서 효율성을 높였다. 또한 안전성을 증명할 수 있는 CK Model을 적용함으로써 안전성을 증명하였으며, 메시지에 인증자를 적용하는 대신에 사용자와 네트워크 사이에 명시적인 상호 인증을 제공한다. 그러나 완전한 전방향 안전성을 제공하지 않으며, 부분적인 전방향 안전성만을 제공한다.

3.2 이기종 네트워크에서 인증 방식

최근 연구는 All-IP 개념 하에 이기종 네트워크를 유지하는 방향이 언급되고 있다. 예를 들어 현재 세계 표준 발의는 Wireless LAN과 3G 네트워크간의 상호 작용에 대하여 명시하고 있으며, 이러한 시나리오에서 스마트카드는 프로토콜 스택의 하위 레이어에서 강력한 인증을 수행할 수 있는 디바이스이다. 따라서 본 방식은 안전한 전자 지불을 위한 새로운 참조 모델과 응용 시나리오를 제안하였다[12]. 결과적으로 3G 네트워크와 Wireless LAN간의 상호 연동 시나리오를 제안하였고, 스마트카드를 이용한 하위 레이어에서의 강한 인증을 제공하였다. 그러나 상위 레벨에서의 상호 인증은 제공되지 않아 유연성의 문제가 있으며, 로밍이 고려되지 않아 이기종 네트워크에서 효율성이 저하되는 단점이 있다.

3.3 이기종 접근을 위한 인증 방식

현재의 인터넷 접근 프로토콜은 대칭키와 공개키

기술을 모두 지원하지 않으며, 유연성 있는 접근 기술과 DoS 공격 및 부인봉쇄를 제공하지 못한다. 또한 다양한 접근 방법 및 네트워크 토플로지에 대하여 제한적이다. 따라서 이기종 접근을 위한 인증 방식에서는 이기종 네트워크 접근을 위한 PANA/IKEv2 인증 프로토콜을 제안하여, 유비쿼터스 이동성을 지원하는 이기종 인터넷 접근 환경에서 사용할 수 있도록 하였다[13]. PANA(Protocol for carrying Authentication for Network Access)는 네트워크 레이어에서 인증을 수행하는 프로토콜로서 IP 기반의 환경에서 링크 프로토콜에 상관없이 인증을 수행할 수 있도록 설계한 프로토콜이다. 이기종 네트워크 접근을 위한 유연하고 확장성 있는 PANA/IKEv2 인증 프로토콜을 제안하였으며, IKEv2로부터 파생되어 대칭키 방식과 공개키 방식 모두 지원 가능하다. 또한 EAP/IKEv2를 기반으로 하여 기존 IKEv2 구조에서 사용 가능하며, Identity 기밀성과 무결성을 지원하고 전방향 안전성을 제공한다. 그리고 중간자 공격, 전수 공격, 재전송 공격, DoS 공격, 사전 공격 등에 안전하다. 그러나 EAP/IKEv2 버전 교섭을 지원하기 위한 메커니즘을 명세하지 않으며, 서비스 위협에 대한 명세가 없다.

4. 제안 방식

유비쿼터스 환경에서 언제 어디서나 정보를 제공받기 위해서는 이기종 네트워크간의 통신 및 디바이스간의 데이터 전송이 가능해야 한다. 그러나 동종 네트워크간 통신에는 기존 보안 기술이 적용되나 이기종 네트워크로 넘어가는 부분에 있어 데이터의 기밀성, 무결성, 인증 등 보안 서비스에 대한 여러 가지 취약점이 발생할 수 있다. 이로 인해 이기종 네트워크간의 통신에 있어 다양한 보안 기술이 적용되어야 하나 기존 기술로는 이기종 네트워크에 접목하기에 적합하지 않다. 따라서 이기종 네트워크에서 데이터의 암호화, 인증 및 키 관리 기술이 새롭게 제시되어야 함에 따라 제안 방식은 그림 1과 같이 이기종 네트워크간의 키 관리를 위해서 키 관리 서버간에 이기종 네트워크간의 대칭키를 설립한다. 기존의 동종 네트워크에서는 디바이스간 키 설립을 직접 설정할 수 있으나, 이기종 네트워크에서는 서로 다른 메커니즘과 전송방식을 사용하는 네트워크간의 통신이기 때문에 이를 해결하기 위하여 서버간의 키 설립 단계에서 보안 협상 및 서버간 키 설립이 이루어진다. 그 후 디바이스는 홈 네트워크 키 관리 서버로부터 인증을 받고, 디바이스간 안전한 통신을 위한 키 설립에 이용될 비밀 값을 분배 받는다. 디바이스들은 분배받은 키를 바탕으로 ID 기반 공개키를 설립하여 안전하고 효율적인 통신을 할 수 있다[14]. 이기종 네트워크에서는 디바이스간 통신이 직접 이루어지기 어렵기 때문에 서버간 키 설립 및 키 관리 서버로부터 인증과 비밀 값 분배가 필요하다.

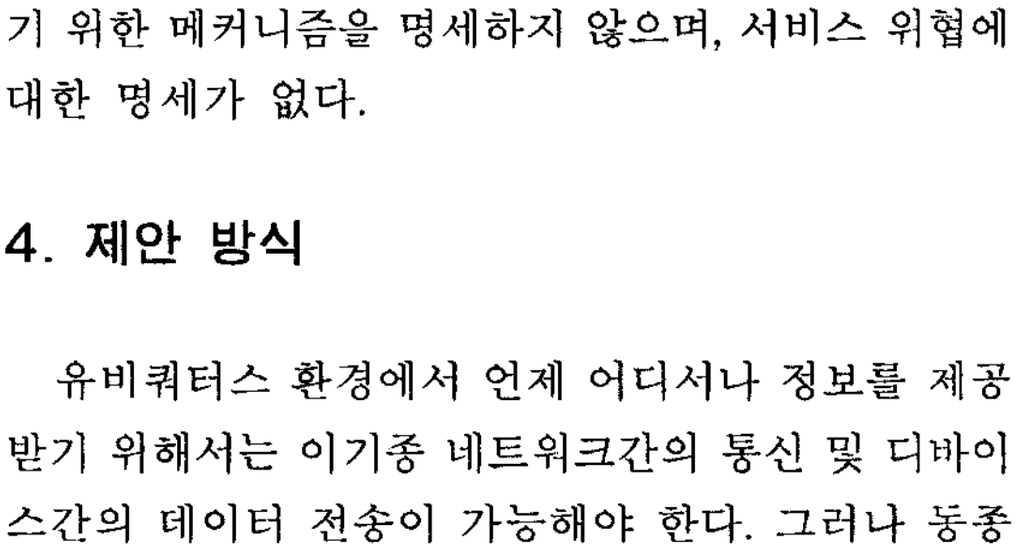

그림 1. 제안 방식 전체 흐름도

4.1 시스템 계수

- 본 제안 방식에서 사용되는 시스템 계수는 다음과 같다.
- * : 각각의 개체 (*KMS* : 키 관리 서버, *Device* : 사용자의 디바이스)
- ID_* : *의 아이디
- PW : 사용자의 디바이스 패스워드
- $h(\ )$: 안전한 일방향 해쉬 함수
- g : 곱셈군 Z_n^*의 생성자
- KEV : 키 관리 서버간 키 설립을 위한 교환 값
- OTP : 일회용 패스워드
- ATV : 인증 시간 값
- SA : 보안 협상 값
- Si : 세션에서 인증을 위한 확인 값
- SV : 세션에서 인증을 위한 비밀 값
- RN_* : *이 생성한 랜덤 수
- $E_*[\ ]$: *의 키로 암호화
- KU_* : *의 공개키
- KR_* : *의 개인키
- KS : 키 관리 서버간의 사전 공유키

- *SK* : 이기종 디바이스간 설립한 세션키
- *HNK* : 이기종 네트워크 간의 대칭키

4.2 제안 프로토콜

제안 프로토콜은 서버간 키 설립, 인증 및 키 분배, 그리고 이기종 디바이스간 키 설립 단계로 이루어지며, 키 관리 서버간의 대칭키와 인증 및 키 분배 단계에서 사용되는 사용자 패스워드는 사전에 분배 되었다고 가정한다.

가. 서버간 키 설립

서버간 키 설립 단계는 보안 협상 및 이기종 네트워크에서 디바이스간의 키 설립에 필요한 이기종 네트워크 대칭키를 교환한다. 키 설립은 Diffie-Hellman 키 교환 방식을 이용하여 설립하며, 통신에 사용되는 *KS*는 키 관리 서버간 사전에 분배되었다고 가정한다.

Step 1. A 네트워크의 키 관리 서버는 사전에 공유한 대칭키 *KS*에 ATV_A(*KMS*$_A$의 *Authentication Time Value*)를 XOR 연산하여 KEV_{KMS_A}(*Key Exchange Value*) 값을 생성한다. 그 후 KMS_B의 공개키를 이용하여 보안 협상과 곱셈군 Z_n^*의 생성자에 g에 KEV_{KMS_A}를 지수승 연산한 값을 암호화 하여 전송한다.

$$KEV_{KMS_A} = KS \oplus ATV_{KMS_A}$$

$$E_{KU_{KMS_B}}[SA,\ g^{KEV_{KMS_A}}]$$

Step 2. B 네트워크의 키 관리 서버 역시 KEV_{KMS_B}를 생성하여 KMS_A의 키 관리 서버의 공개키로 보안 협상과 곱셈군 Z_n^*의 생성자에 g에 KEV_{KMS_B}를 지수승 연산한 값을 암호화 하여 전송한다. 그 후 자신이 생성한 값과 KMS_A로부터 전송받은 값을 지수승 연산하여 이기종 네트워크 대칭키를 설립한다.

$$KEV_{KMS_B} = KS \oplus ATV_{KMS_B}$$

$$E_{KU_{KMS_B}}[SA,\ g^{KEV_{KMS_B}}]$$

$$HNK = (g^{KEV_{KMS_A}})^{KEV_{KMS_B}}$$

나. 인증 및 키 분배

인증 및 키 분배 단계는 키 관리 서버간의 키 설립이 완료된 이후, 키 관리 서버는 자신의 네트워크에 속해 있는 디바이스를 인증하고 설립된 이기종 네트워크 대칭키를 디바이스에게 전송한다. 디바이스는 전송받은 키를 이용하여 디바이스간의 통신에서 사용할 키를 설립하게 되며, 각 개체간의 인증은 *OTP*를 이용하여 상호 인증을 제공한다. 본 단계에서 $Device_A$와 $Device_B$는 동일한 과정을 수행하므로, $Device_A$의 인증 및 키 분배 과정만을 나타낸다.

Step 1. $Device_A$와 KMS_A는 g에 자신의 아이디를 지수승 연산하여 공개키를 생성하고 *Random Nmber*를 이용하여 개인키를 생성한다. 그 후 자신의 패스워드에 해쉬된 ATV_{Device_A}를 XOR 연산하여 OTP_{Device_A}를 생성하고, 키 관리 서버의 공개키로 해쉬된 ATV_{Device_A}와 OTP_{Device_A}를 KMS_A의 공개키로 암호화 하여 ID_{Device_A}와 함께 전송한다.

$$KU_{Device_A} = g^{ID_{Device_A}},\ KR_{Device_A} = (g^{ID_{Device_A}})^{RN_{Device_A}}$$

$$KU_{KMS_A} = g^{ID_{KMS_A}},\ KR_{KMS_A} = (g^{ID_{KMS_A}})^{RN_{KMS_A}}$$

$$OTP_{Device_A} = PW \oplus h(ATV_{Device_A})$$

$$ID_{Device_A},\ E_{KU_{KMS_A}}[h(ATV_{Device_A}), OTP_{Device_A}]$$

Step 2. KMS_A는 $Device_A$가 전송한 값을 복호화 한 다음 자신의 데이터베이스에 저장된 사용자의 패스워드와 $h(ATV_{Device_A})$를 XOR 연산하여 OTP_{Device_A}'를 생성하고 전송된 OTP_{Device_A}와 비교하여 값이 일치하면 사용자를 인증한다. 인증이 완료되면, 키 관리 서버는 사용자의 패스워드에 $h(ATV_{KMS_A})$를 XOR 연산하여 OTP_{KMS_A}를 생성하고 $h(ATV_{KMS_A})$와 서버간 키 설립 단계에서 설립한 이기종 네트워크 대칭키를 $Device_A$의 공개키로 암호화 하여 전송한다.

$$OTP_{Device_A}' = PW \oplus h(ATV_{Device_A})$$

$$OTP_{Device_A} \stackrel{?}{=} OTP_{Device_A}'$$

$$OTP_{KMS_A}' = PW \oplus h(ATV_{KMS_A})$$

$$E_{KU_{Device_A}}[h(ATV_{KMS_A}), OTP_{KMS_A}, HNK]$$

다. 이기종 디바이스간 키 설립

각 디바이스들은 자신의 ID 기반 개인키와 공개키 쌍을 생성하고 세션 식별 값과 세션 값을 이용해 상

호 인증을 한다. 디바이스들의 개인키와 공개키, 그리고 통신에 사용되는 파라미터를 통해 세션키를 설립하고, 설립된 세션키를 통해 이기종 디바이스간의 안전한 통신을 할 수 있다. 키 설립의 기본적인 개념은 Bilinear Pairing의 Admissible Bilinear Map을 기반으로 한다.

Step 1. $Device_A$와 $Device_B$는 g에 자신의 아이디를 지수승 연산하여 공개키를 생성하고 *HNK*를 이용하여 개인키를 생성한다. 그 후 $Si_{Device_A}(Session\ identifier)$ 값과 $SV_{Device_A}(Session\ Value)$를 생성하여 ID_{Device_A}와 함께 전송한다.

$$KU_{Device_A} = g^{ID_{Device_A}},\ KR_{Device_A} = g^{ID_{Device_A}} \bullet HNK$$

$$KU_{Device_B} = g^{ID_{Device_B}},\ KR_{Device_B} = g^{ID_{Device_B}} \bullet HNK$$

$$Si_{Device_A} = ATV_{Device_A} \bullet g^{ID_{Device_A}}$$

$$SV_{Device_A} = e(KR_{Device_A},\ ATV_{Device_A} \bullet KU_{Device_B})$$

$$ID_{Device_A}, Si_{Device_A}, SV_{Device_A}$$

Step 2. $Device_B$는 개인키와 전송된 Si_{Device_A}를 연산하여 SV_{Device_A}'를 생성하고 전송된 SV_{Device_A}와 비교하여 값이 일치하면 사용자를 인증한다. 인증이 완료되면 Si_{Device_B}를 생성하여 자신의 개인키, 그리고 Si_{Device_A}를 연산하여 세션키(*SK*)를 생성한 다음 암호화 하여 ID_{Device_A}와 Si_{Device_B}를 $Device_A$에게 전송한다.

$$SV_{Device_A}' = e(KR_{Device_B},\ Si_{Device_A})$$

$$SV_{Device_A} \stackrel{?}{=} SV_{Device_A}'$$

$$Si_{Device_B} = ATV_{Device_B} \bullet g^{ID_{Device_B}}$$

$$SK = e(KR_{Device_B},\ Si_{Device_A} \bullet Si_{Device_B})$$

$$ID_{Device_B}, Si_{Device_B}, E_{SK}[SK]$$

Step 3. $Device_A$는 $Device_B$로부터 전송된 값으로 *SK'*를 생성한 다음 복호화된 *SK*와 비교하여 값이 일치하면 $Device_B$를 인증하고 세션키 *SK*를 검증한다. 이후의 디바이스간의 통신은 설립된 *SK*를 통하여 안전하게 통신한다.

$$SK' = e(KR_{Device_A} \bullet Si_{Device_B},\ ATV_{Device_A} \bullet KU_{Device_B})$$

$$SK \stackrel{?}{=} SK'$$

5. 제안 방식의 분석

제안 방식의 프로토콜을 안전성 및 효율성에 대하여 분석하고, 총 통신 횟수 및 초기 인증 통신 횟수에 대하여 성능 비교를 통해 분석한다.

5.1 안전성 분석

제안 방식의 프로토콜을 2.1에서 언급한 안전성과 제 3자의 공격에 대한 요구사항에 맞추어 분석하면 다음과 같으며, 기존 방식과의 분석은 표 1과 같다.

- 기밀성(Confidentiality) : 기밀성은 정보를 해석할 수 없도록 암호화를 통해서 이루어진다. 제안 방식은 키 관리 서버간의 대칭키(*HNK*)와 디바이스간의 세션키(*SK*), ID기반 공개키($KU_{Device_A} = g^{ID_{Device_A}},\ KR_{Device_A} = g^{ID_{Device_A}} \bullet HNK$)를 통해 제공된다.
- 무결성(Integrity) : 전송된 데이터를 바로 검증 가능함으로써 무결성이 제공되며, 메시지의 해쉬 값($h(ATV_{Device_A})$)을 통해 제공된다.
- 인증(Authentication) : 제안 방식에서는 디바이스가 키 관리 서버에게 OTP_{Device_A}를 전송함으로써 제공되고, 키 관리 서버가 디바이스에게 $OTP_{KMS_A} = PW \oplus h(ATV_{KMS_A})$를 전송함으로써 제공된다. 디바이스간의 인증은 Si_{Device_A}와 SV_{Device_A}를 검증함으로써 제공된다.
- 접근제어(Access Control) : 불법적인 사용자는 서비스에 접근할 수 없어야 한다. 정당하게 인증받지 않은 사용자는 키 관리 서버로부터 이기종 네트워크 키를 분배 받을 수 없어 키 설립이 불가능하다.
- 부인 봉쇄(Non-repudiation) : 부인 방지는 전자서명에 의해 해결할 수 있으며, 제안 방식은 연산량의 문제로 전자서명을 제공하지 않아 명시적인 부인 봉쇄를 제공하지 못하나, 정당한 키 관리 서버만 값을 생성할 수 있기 때문에 묵시적인 부인 봉쇄를 제공한다.
- 상호 인증(Mutual Authentication) : 이기종 네트워크에서는 다양한 객체간 통신이기 때문에 상호간의 인증이 필요하다. 제안 방식은 디바이스와 키 관리 서버간의 상호 인증(OTP_{Device_A}, OTP_{KMS_A}), 디바이스간의 상호 인증(SV_{Device_A}와

표 1. 제안 방식 안전성 분석표

	기존방식 1 [11]	기존방식 2 [12]	기존방식 3 [13]	**제안방식**
기밀성	○	△	○	○
	공개키/세션키	MAC/대칭키	공개키/세션키	**대칭키/ID 기반 공개키**
무결성	○	○	○	○
	해쉬함수	MAC	Identity무결성 제공	**해쉬 함수**
인증	○	○	○	○
	ID기반 공개키	AUTH1/AUTH2	AUTH/CERT	**OTP/Si/SV**
접근제어	○	○	○	○
	인증을 받지 않은 사용자는 서비스를 제공받을 수 없음			
부인봉쇄	○	△	○	△
	전자서명	Session ID	전자서명	**묵시적 제공**
상호 인증	△	△	○	○
	사용자와 홈 서버간의 상호 인증만 제공	MN과 H-AAA간의 상호 인증만 제공	AUTH 구성요소의 ID 확인으로 제공	**디바이스와 키 관리 서버간/ 디바이스간 상호인증 제공**
단대단보안	○	○	△	○
	종단간 메시지 암호화		**종단간 메시지 암호화**	
도청공격	△	△	○	○
	통신로 상의 메시지 노출로 인한 도청공격의 가능성 존재		비밀 값을 유출할 수 없음	
재전송 공격	○	○	○	○
	Nonce	Nonce	Sequence Number	**OTP/ATV**
위장 공격	○	△	○	○
	전자서명		전자서명(Option)	**상호인증**
패스워드 추측 공격	○	△	○	○
	패스워드 추측 불가	중요정보 난수노출	패스워드 추측 불가	**패스워드 추측 불가**
효율성	△	△	△	○
	완전한 전방향 안전성 제공 못함	유연성문제/ 로밍에 대한 문제	유연성제공/연산량 및 메시지 횟수증가	**연산량 감소/인증 단계에서 효율성 문제**

[○:제공,안전 △:보통 X:제공못함, 안전하지 않음]

*SK*를 검증) 모두를 제공한다.

- 단대단 보안(End-to-End Secrecy) : 이기종 네트워크에의 단말간 통신은 단대단 보안이 제공되어야 한다. 제안 방식에서는 종단간 뿐만 아니라 단대단 보안까지 제공함으로써 안전성을 강화 시켰다.
- 도청 공격(Eavesdropping Attack) : 도청 공격에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 비밀 값을 유추할 수 없도록 해야 한다. 암호화 통신을 하기 때문에 도청 공격으로부터 안전하다.
- 재전송 공격(Replay Attack) : 제안 방식은 인증 및 키 분배 단계에서는 *OTP*와 *ATV*로 안전하며, 이기종 디바이스간 키 설립 단계에서는 *Si*와 *SV*로 안전하다.
- 패스워드 추측 공격(Password Guessing Attack) : 통신 중에 전송 되는 메시지를 분석하여 패스워드를 추측하는 것을 막아야한다. 사용자를 인증하는 실제적인 값은 패스워드가 아니라 *OTP*이기 때문에 *OTP*에서 패스워드의 추측은 불가능하다. 이는 패스워드와 *ATV*를 XOR 연산을 하고, 키 관리 서버의 공개키로 암호화하기 때문에 메시지에 대한 분석을 하여도 패스워드를 추측 공격에 안전하다.

표 2. 통신에 따른 효율성 분석표 (S : 대칭키 암호화 연산, P : 공개키 암호화 연산, n : 지역 인증 서버의 수)

	기존방식 1 [11]	기존방식 2 [12]	기존방식 3 [13]	**제안방식**
총 통신 횟수	5 회	12 회	18 회	**8 회**
초기 인증 통신 횟수	5 회	12 회	10 회	**2 회**
암호화 연산	P : 3 회	0 회	S : 2 회	**P : 3 회 (ID 기반 공개키)**
해쉬 연산	2 회	0 회	2 회	**3 회**
MAC 연산	3 회	3 회	2 회	**0 회**
지수승 연산	0 회	0 회	0 회	**6 회**
보유키 개수	n+2 개	n+1 개	n*3 개	**2 개**

- 위장 공격(Impersonation Attack) : 제 3자가 정당한 사용자처럼 접근하는 것을 막아야 한다. 제안 방식은 각 단계마다 상호 인증을 제공하기 때문에 위장 공격이 불가능하다.

5.2 효율성 분석

제안 방식의 프로토콜을 통신에 따른 효율성에 관하여 분석하면 다음과 같다.

- 통신에 따른 효율성 : 통신에 따른 효율성 분석은 표 2와 같다. 제안 방식의 총 통신 횟수는 서버간 키 설립 단계, 인증 및 키 분배 단계, 디바이스간 키 설립 단계까지 모두 포함한 것이기 때문에 기존 방식의 인증 단계만의 횟수와 비교하였을 때 큰 차이로 감소시킨 것이다. 또한 초기 인증 통신 횟수도 기존 방식에 비해 월등히 감소하여, 이기종 네트워크 키 설립 시 지연을 감소시켰다. 암호화 연산에서 제안 방식은 공개키 연산이 3회이나, 이 연산은 ID 기반 공개키 연산이기 때문에 기존의 인증서 기반 공개키 연산에 비해 효율적이며, MAC(Message Authentication Code)연산에서는 0회로 감소시켰으나 기존 방식에 비해 지수승 연산이 많은 것은 향후 보완해야할 것으로 사료된다. 그리고 마지막으로 보유키 개수에서 ID 기반 공개키 사용으로 키 관리의 문제점을 해결하였다.
- 효율성(Efficiency) : 본 방식은 이기종 네트워크간의 안전한 키 관리 프로토콜을 제안하였으며, 키 설립단계에서 ID 기반 공개키 방식을 사용하여 기존의 공개키 방식보다 연산량이 적고 효율적이다. 일반적인 공개키 방식은 키 관리 서버간의 통신에서 사용되기 때문에 사용자의 연산량에는 영향을 주지 않는다. 키 관리 서버와의 인증 단계 및 디바이스간의 통신에서도 디바이스가 ID 기반 공개키 방식을 사용하여 효율성을 제공한다.

5.3 비용 분석

제안 방식과 기존 방식의 비용 분석을 위해 표 2의 초기 인증 통신 횟수 및 암호화 연산 메시지를 통해 비교한다. 인증 횟수의 감소 및 암호화 연산에 따른 성능을 비교하기 위해 초기 인증 통신 횟수는 a로, 암호화 연산 횟수를 e(암호화 연산 횟수 e에서 인증서 기반 공개키 연산은 $2e$, 대칭키 연산 및 ID 기반 공개키 연산은 e)로 정의하며, 인증 메시지 비용은 $c1$, 암호화 연산 비용은 $c2$로 정의한다. 따라서 성능 비교를 구하기 위한 수식은 $Total\ Cost = a \cdot c1 + e \cdot c2$ 와 같다. 인증 메시지 비용 $c1$은 1씩 증가하고, 암호화 연산 비용 $c2$는 2씩 증가하는 것으로 가정한다. 이는 인증 메시지를 생성하는 비용보다 암호화 연산

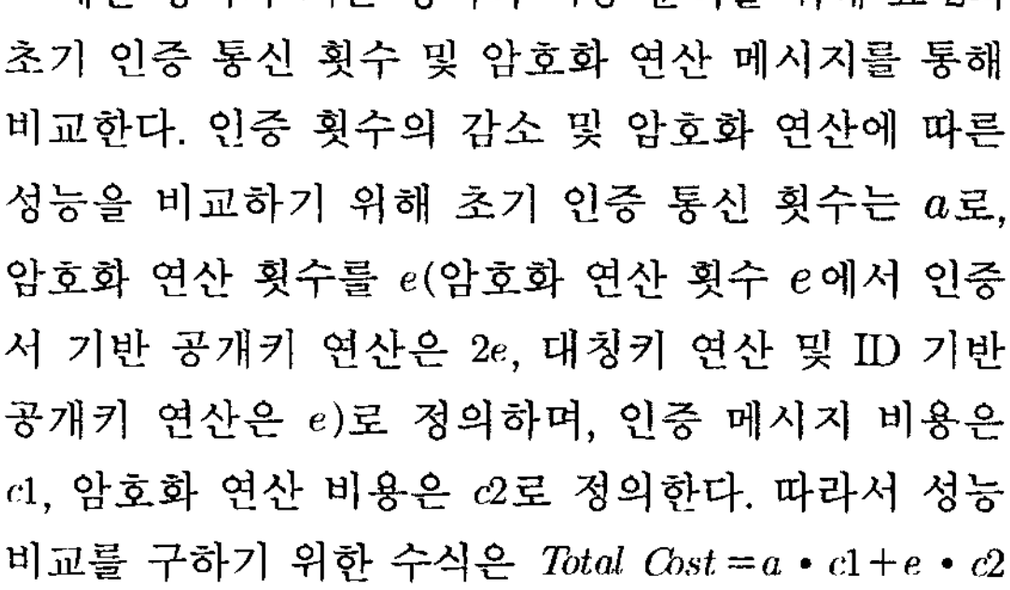

그림 2. 기존 방식과 제안 방식의 성능 비교

에 드는 비용이 더 높을 것으로 가정한 것이다. 통신에 따른 효율성 분석표에서 초기 인증 통신 횟수 및 암호화 연산을 수식에 적용하면, 기존 방식 1의 *Total Cost* $=5\alpha+6\beta$과 같으며, 제안 방식의 *Total Cost* $=2\alpha+3\beta$와 같다. 따라서 *Message Cost*에 따른 *Total Cost*를 구하면 다음 그림 2와 같다. 그림에서 보듯이 제안 방식은 기존 방식에 비해 좋은 성능을 보이며, 기존 방식 2는 암호화 연산이 없기 때문에 초기 인증 통신 횟수에 따른 비용만 산출하여 성능을 비교하였다.

6. 결 론

유선 네트워크의 빠른 전송속도 및 다양한 서비스와 무선의 편리성 및 이동성이 결합되어 새로운 서비스 영역을 창출하고 사용자와 서비스 제공자 모두에게 새로운 변화를 가져올 신기술로 유/무선 통합 시대가 전개되고 있다. 유/무선 통합 서비스 중에서 네트워크의 통합은 이종 네트워크간 연동에 의한 네트워크 융합과 네트워크상에서 전송기술간 융합으로써 매주 중요한 부분을 차지하고 있다. 이기종 네트워크의 융합은 서로 다른 네트워크의 융합으로 인해 기존의 보안 기술 및 통신 기술을 그대로 적용하기가 매우 어려우며, 보안 측면에서도 많은 취약점을 내포하고 있다.

본 연구에서는 이기종 네트워크의 요구 사항 및 보안 취약점을 보완하고자 이기종 네트워크에서 공개키를 이용한 이기종 네트워크간의 안전하고 효율적인 키 관리 기술에 관한 연구를 진행하였다. 이기종 네트워크간의 키 관리 기술에 대한 제안 방식은 키 관리 서버간에 이기종 네트워크 대칭키를 설립한다. 그 후 키 관리 서버는 자신의 도메인에 속해있는 디바이스에게 키를 분배하고 디바이스들은 키를 바탕으로 ID 기반 공개키를 설립하여 안전한 통신을 할 수 있다. ID 기반 공개키 방식을 사용함으로써 디바이스의 연산량을 감소 시켰으며, 효율성을 증가 시켰다. 그러나 ID기반 공개키 방식을 사용하더라도 지수승 연산의 사용으로 연산량에 문제가 될 수 있으며, 이에 따라 향후 경량화된 ID 기반 공개키 방식의 적용이 필요할 것이며, 디바이스의 이기종 네트워크의 이동 및 이기종 디바이스간의 보안방안에 대한 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] Dong-Hoon Yang, Seongcheol Kim, Changi Nam, and Ji-Sook Moon, "Fixed and mobile service convergence and reconfiguration of telecommunications value chains," *IEEE Wireless Communications*, Vol. 11, Issue. 5, 2004.

[2] 박형수, 이형우, 이동훈, "이기종 무선 이동망간 통합 인증 및 키 관리 기법," 전자공학회논문지, Vol. 43, TC No. 7, pp. 50-59, 2006.

[3] 서승현, 조태남, 이상호, "OTP-EKE : 원-타임-패스워드 기반의 키 교환 프로토콜," 한국정보과학회논문지, pp. 291-298, 2002.

[4] 이상억, "ID 기반의 단말간 무선랜 인증," 경북대학교 대학원, 2004.

[5] 최용락, 소우영, 이재광, 이임영, 컴퓨터 통신보안, 도서출판그린, 2005.

[6] IP Security Protocol(IPSec), IETF, http://www.ietf.org/html.charters/

[7] Dan Harkins, and Dave Carrel, "The Internet Key Exchange(IKE)," RFC 2409, 1998.

[8] 임수현, 박용진, "인터넷 키 관리 프로토콜 IKE와 IKEv2 에 관한 비교연구," 한국정보과학회 가을 학술발표논문집 Vol. 30, No. 2, 한양대학교, 2003.

[9] 김한철, "IPSec 의 키 관리 프로토콜에 관한 연구," 동의대학교, 2003.

[10] Adi Shamir, "Identity-based cryptosystems and signature schemes," *CRYPTO'84*, pp. 47-53, 1984.

[11] Jun Jiang, Chen He, and Ling-ge Jiang, "On the Design of Provably Secure Identity-Based Authentication and Key Exchange Protocol for Heterogeneous Wireless Access," *ICCNMC*, pp. 972-981, 2005.

[12] Joaquín Torres, Antonio Izquierdo, Arturo Ribagorda, and Almudena Alcaide, "Secure Electronic Payments in Heterogeneous Networking: New Authentication Protocols Approach," *ICCSA*, pp. 729-738, 2005.

[13] Paulo S. Pagliusi and Chris J. Mitchell,

"PANA/IKEv2 : an Internet Authentication Protocol for Heterogeneous Access," *WISA 2003*, pp. 135-149, 2003.

[14] 문종식, 이임영, "유비쿼터스 환경에서 이기종 네트워크간의 안전한 키 관리 기술에 관한 연구," 정보보호학회 하계학술대회 논문집, 제 17권 제1호, pp. 162-165, 2007.

문 종 식

2006년 2월 순천향대학교 정보기술공학부 졸업
2008년 2월 순천향대학교 전산학과 석사
2008년 3월~현재 순천향대학교 컴퓨터학과 박사 과정
관심분야 : AAA, 이기종 네트워크

이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학 전공 석사
1989년 3월 오사카대학 통신공학 전공 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 컴퓨터 학부 교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안